UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A BLACK IPHONE 12, IMEI # 352590374630790, IN AN EVIDENCE PACKAGE IN THE POSSESSION OF USPS-OIG SA JUSTIN LYNCH IN THE DISTRICT OF DELAWARE

Case No. 22-203M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of Delaware, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 1709	Theft of Mail Matter by Postal Employee

The application is based on these facts:

see attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Justin Lynch, USPS-OIG

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/10/2022

Judge's signature

City and state: Wilmington, Delaware

Honorable Sherry R. Fallon, U.S. Magistrate Judge

Printed name and title

Print Save As... Attach Reset

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF: A BLACK IPHONE 12, IMEI NUMBER 352590374630790, CURRENTLY IN AN EVIDENCE PACKAGE IN THE POSSESSION OF USPS-OIG SA JUSTIN LYNCH IN THE DISTRICT OF DELAWARE	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent Justin Lynch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a black iPhone 12 with IMEI number 352590374630790 (the "Subject Device"), stored in an evidence package in the possession of USPS-OIG SA Justin Lynch in the District of Delaware, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the U.S. Postal Service – Office of Inspector General ("USPS-OIG"). I have been a Special Agent of the USPS-OIG since September 2019. Prior to serving as a Special Agent with USPS-OIG, I was employed as Special Agent with the U.S. Treasury Inspector General for Tax Administration ("TIGTA") for approximately five years. As a Special Agent with USPS-OIG and TIGTA, I have participated in numerous investigations involving allegations of mail theft and fraud, bank fraud, and identity theft. I have also participated in executing search warrants in investigations related to mail theft and fraud, bank fraud, and identity theft, and executed search warrants involving the search and seizure of

financial documents and records and electronic media, including cellular telephones and laptop computers. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. As discussed below, there is probable cause to believe that Jasmine Holloway has violated Title 18, United States Code, Section 1709 (Theft of Mail Matter by Postal Employee). There is also probable cause to search the Subject Device for evidence, fruits, and instrumentalities of that crime.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

I. Investigative Background

5. ("Company 1") has filed a series of complaints with the United States Postal Inspection Service (USPIS) and United States Postal Service Office of Inspector General (USPS-OIG) stating it was the victim of ongoing theft.

6. On October 15, 2021, your affiant conducted a consensual interview with Company 1's operations manager ("Witness 1"), who explained Company 1 is a shipping logistics company. Customers purchase items, typically electronics like smartphones and laptops, to be shipped to former Soviet-bloc countries. Customers ship the items to Company 1's warehouse in either Port Reading, New Jersey or Wilmington, Delaware, and then Company 1

ships the items overseas. Customers submit descriptions of items being shipped to Company 1 through Company 1's website.

7. Witness 1 explained that approximately two years ago Company 1 started receiving damaged, empty boxes. This began sporadically but ramped up in 2021. On August 9, 2021, Witness 1 began a spreadsheet logging every empty parcel received from that date going forward, including the parcel's tracking number, the date Company 1 received the empty parcel, and a link to an image of the empty packaging. All empty packages were delivered to Company 1's Wilmington, Delaware warehouse and came through the USPS Marshallton Branch ("Marshallton Post Office") located at 3434 Old Capitol Trail, Wilmington, Delaware 19808. Company 1 recorded over 150 empty parcels received from August 9, 2021-October 15, 2021, and Witness 1 confirmed they receive more empty packages every day.

8. Witness 1 later informed your affiant that in addition to the at least 150 empty parcels that had been delivered to date by USPS to Company 1's Wilmington, Delaware warehouse, Company 1 had a list of 45 additional parcels that were never received in their entirety, despite USPS tracking information indicating those parcels were delivered. Some of these parcels contained smartphones, one of which (a black iPhone 12) was subsequently identified by your affiant as being used in Philadelphia, Pennsylvania.

9. On October 22, 2021, your affiant conducted a consensual interview of the customer service manager of the Marshallton Post Office ("Witness 2"). Witness 2 confirmed that the Marshallton Post Office receives approximately 1,000 parcels a day addressed to Company 1. While those packages receive no special processing, they are stored in a separate area of the post office given their volume. Marshallton Post Office receives parcels for

Company 1 seven days a week; however, Company 1's Wilmington, DE warehouse is only open Monday through Friday. Thus, parcels received for Company 1 at Marshallton Post Office on the weekend sit onsite all weekend and are not delivered until the following Monday morning.

10. Your affiant knows from training and experience that when a package arrives at a post office, it is scanned as "arrival at unit." USPS takes and maintains photographs of parcels as they arrive at the post office. Your affiant reviewed images from the Marshallton Post Office and confirmed that a large percentage of the parcels which arrived at Company 1 damaged and empty had arrived at the Marshallton Post Office intact, meaning they were emptied and damaged sometime after their arrival at the Marshallton Post Office. Your affiant also reviewed a USPS database and determined that the majority of parcels which arrived at Company 1 damaged and empty had arrived at the Marshallton Post Office on a Sunday.

11. Your affiant worked with others at USPS-OIG to install covert surveillance cameras to capture the area where Company 1's packages are stored at the Marshallton Post Office. The surveillance cameras record seven days a week from approximately 2:45 am to 9:00 pm (Marshallton Post Office's operating hours are approximately 3:00 am to 8:00 pm). On January 7, 2022, your affiant reviewed footage from December 12, 2021 and discovered that parcels that were in view of the cameras at 9:00 pm had disappeared when the cameras restarted at 2:45 am the next morning. In addition, a light in the janitor's closet that was turned on on December 12, 2021 at 9:00 pm was off the next day at 2:45 am. Your affiant contacted USPIS' National Law Enforcement Communication Center (NLECC), which serves as a dispatch center for USPS' law enforcement agencies, to inquire about Marshallton Post Office's security alarm on the night of December 12, 2021. NLECC advised Marshallton Post Office's security system

was disarmed that night at 11:00 pm and reactivated 43 minutes later, confirming someone had entered the post office that night.

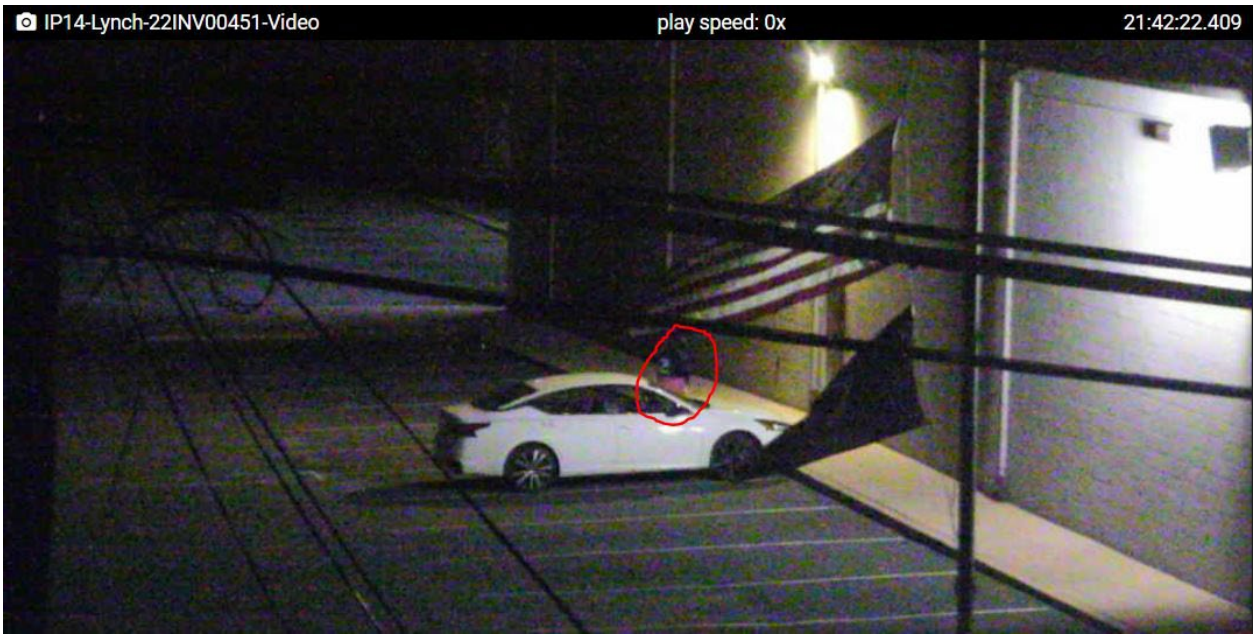
12. On January 8, 2022, your affiant obtained from NLECC and reviewed the Marshallton Post Office Alarm Panel Log dating back to August 1, 2021 (which covered the span of Company 1's empty parcel log). Your affiant discovered an unknown individual(s) had accessed Marshallton Post Office overnight at least 35 times from August 2021 to January 2022, usually on Sundays. An alarm code belonging to "User 3" was exclusively used to deactivate and reactivate the Marshallton Post Office alarm panel those nights. SA Lynch searched USPS' time and attendance system and did not identify any employees who were clocked in during the overnight intrusions.

13. On or around January 9, 2022, USPS-OIG altered the covert surveillance cameras in Marshallton Post Office to record all night on Sundays. Review of the footage from Sunday, January 9, 2022, revealed an unknown individual entered Marshallton Post Office at 11:26 pm, after disabling the alarm panel with the code for "User 3." The individual immediately went to the area where Company 1's parcels are stored in Marshallton Post Office and began cutting open parcels and removing their contents. The individual opened parcels to steal their contents for over 20 minutes and left at 11:50 pm. While the camera captured the individual's movements, it did not capture the individual in enough detail for identification.

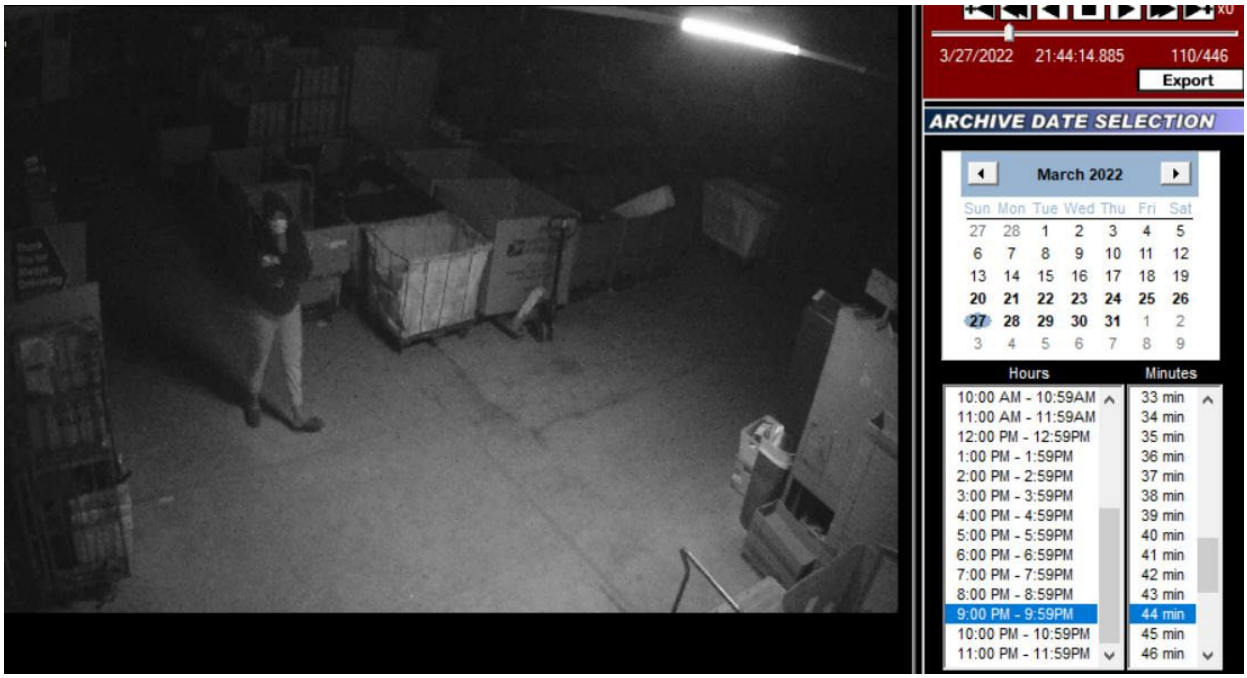
14. Your affiant learned from Witness 2 that the alarm code belonging to "User 3" for Marshallton Post Office is a shared access code used by multiple Marshallton Post Office staff members. Further, anyone who knows the "User 3" code can enter the Marshallton Post Office, even if they are not a current employee.

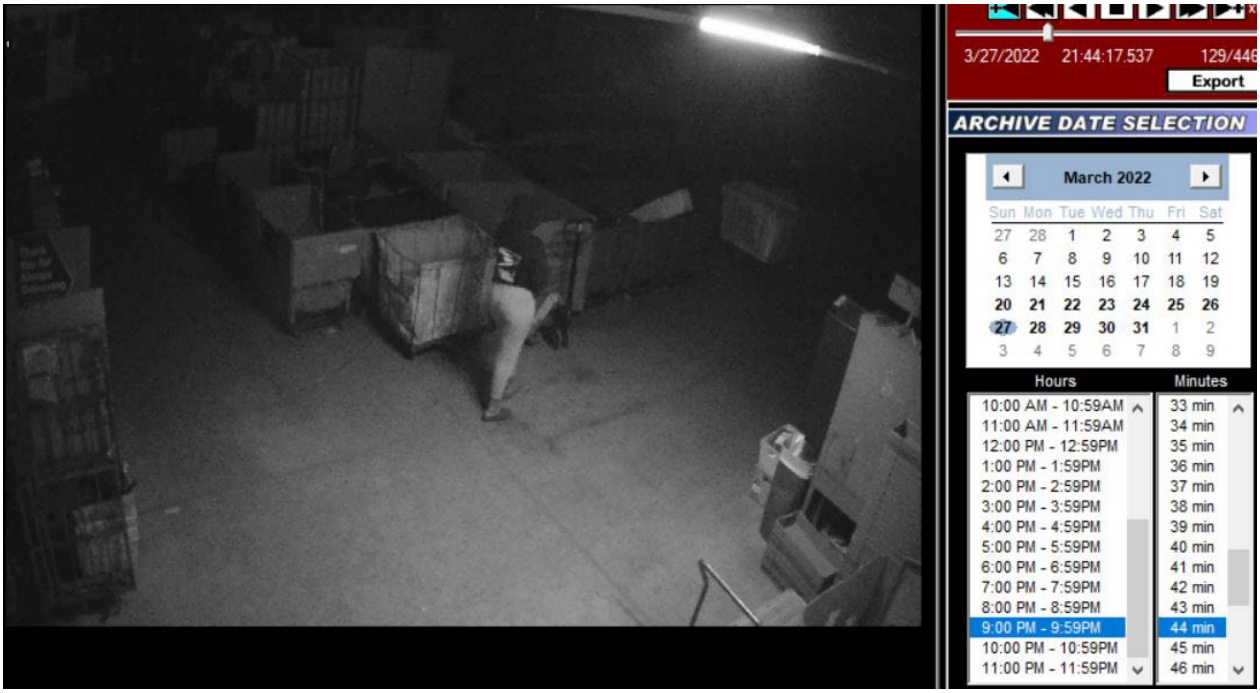
15. On or around January 27, 2022, a pole camera was installed outside Marshallton Post Office to enable exterior surveillance of the facility, in an attempt to identify who was entering the building on Sunday evenings.

16. On Sunday, March 27, 2022, the pole camera captured a vehicle that appeared to be a white sixth generation (2019 to present) Nissan Altima arriving at Marshallton Post Office at 9:42 pm:



The vehicle had front and rear license plates (ruling out a registration to Delaware or Pennsylvania), with the front plate appearing to have a white background. An individual who appeared to be a female, wearing pink sweatpants and a dark USPS hooded sweatshirt, exited the vehicle and entered Marshallton Post Office. Review of the covert surveillance cameras inside Marshallton Post Office revealed the unknown female walked towards the area where Company 1's parcels are stored and began opening parcels and taking their contents, see below:





The unknown female opened parcels and removed their contents for approximately 15 minutes, returned to the vehicle parked outside, and left Marshallton Post Office at 9:57 pm.

17. On April 12, 2022, your affiant reviewed the surveillance footage from March 27, 2022 with Witness 2. Witness 2 immediately said, "That looks like Jasmine." Witness 2 identified "Jasmine" as Jasmine Holloway (Holloway), a USPS clerk who worked at Marshallton Post Office from 2019 through March 2021. Witness 2 showed Holloway's Facebook profile to your affiant to point out the physical similarities between Holloway and the female captured on the surveillance footage. Witness 2 also stated he remembered Holloway wearing pink sweatpants to work and the same type of sandals as the female captured on the surveillance footage.

18. Witness 2 stated Holloway's duties as a clerk at Marshallton Post Office included working on Sundays to sort packages (when staffing would have been minimal), and Holloway would have had the alarm code belonging to "User 3" for Marshallton Post Office.

19. Your affiant reviewed Holloway's USPS employee profile and noted her address of record was . On April 13, 2022, your affiant traveled to Holloway's residence and noticed a white sixth generation Nissan Altima bearing white Massachusetts license plates with number 1JJR73 parked in the immediate vicinity of Holloway's residence. Your affiant checked the registration for this vehicle which came back to a 2021 Nissan Altima owned by Avis Rental Car. Your affiant obtained the rental reservation agreement from Avis for the 2021 Nissan Altima, which revealed it was rented from March 20, 2022 to April 18, 2022, by of Philadelphia, Pennsylvania. Your affiant has not yet ascertained the connection between Holloway and .

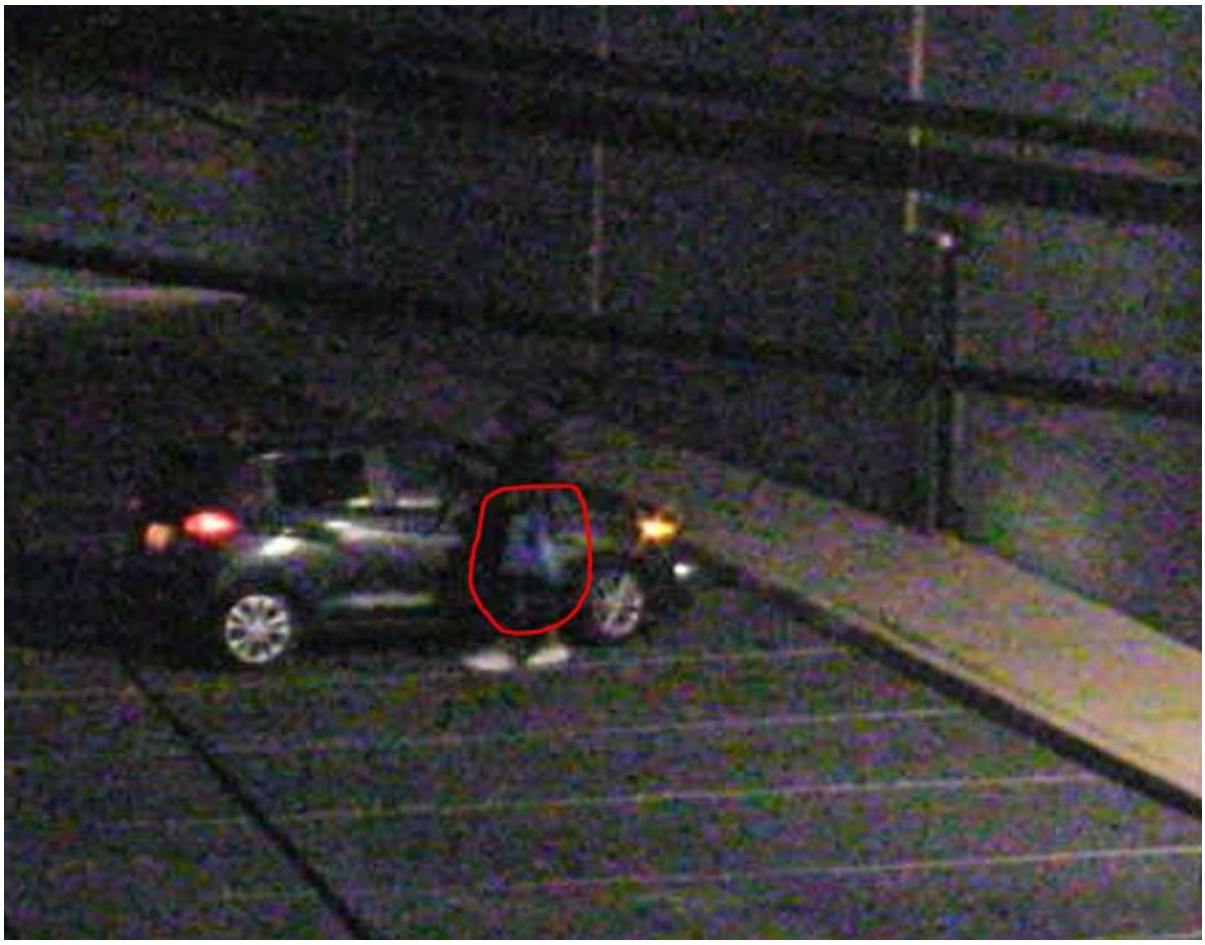
20. On Sunday May 22, 2022, the pole camera captured a dark blue sixth generation Dodge Charger arrive at Marshallton Post Office at 6:00 pm. The vehicle had a Delaware

license plate that was not legible in the footage. An individual consistent with the appearance of Holloway exited the driver's side of the vehicle and entered Marshallton Post Office using the User 3 access code. Review of the covert surveillance cameras inside Marshallton Post Office revealed the individual consistent with Holloway walked towards the area where Company 1's parcels are stored and opened parcels to remove their contents. The female consistent with Holloway opened parcels and removed their contents for approximately 20 minutes, returned to the Dodge Charger carrying what appeared to be a full bag, and left Marshallton Post Office, see below:

21. The pole camera captured the same dark blue Dodge Charger return to Marshallton Post Office at 7:43 pm that night An individual consistent with the appearance of Holloway exited the driver's side of the vehicle and re-entered Marshallton Post Office using the User 3 access code. Review of the covert surveillance cameras inside Marshallton Post Office

revealed the individual consistent with Holloway walked towards the area where Company 1's parcels are stored again and opened parcels to remove their contents. The female consistent with Holloway opened parcels and removed their contents for approximately 10 minutes, returned to the Dodge Charger, and left Marshallton Post Office

22. On Sunday May 29, 2022, the pole camera captured a vehicle that appears to be a dark gray, second generation (2011 to present) Chevrolet Spark arrive at Marshallton Post Office at 8:34 pm. The vehicle appears to have a Pennsylvania license plate that was not legible in the footage. An individual consistent with the appearance of Holloway exited the passenger's side of the vehicle and entered Marshallton Post Office using the User 3 access code. Review of the covert surveillance cameras inside Marshallton Post Office revealed the individual consistent with Holloway walked towards the area where Company 1's parcels are stored and opened parcels to remove their contents. The female consistent with Holloway opened parcels and removed their contents for approximately 20 minutes, returned to the Chevy Spark carrying a blue bag full of items stolen from the post office, and left Marshallton Post Office, see below:



23. On the evening of Sunday, June 5, 2022, USPS-OIG special agents conducted a surveillance operation to monitor the activities of USPS Clerk Jasmine Holloway at Holloway's residence and the Marshallton Post Office. On this date at 8:11 pm, a USPS-OIG special agent witnessed an African American female consistent with Holloway's physical description exit Holloway's residence wearing a mask, dark USPS hooded sweatshirt, white shorts, and carrying a blue bag. The female consistent with Holloway entered a vehicle waiting outside of Holloway's residence and departed the area.

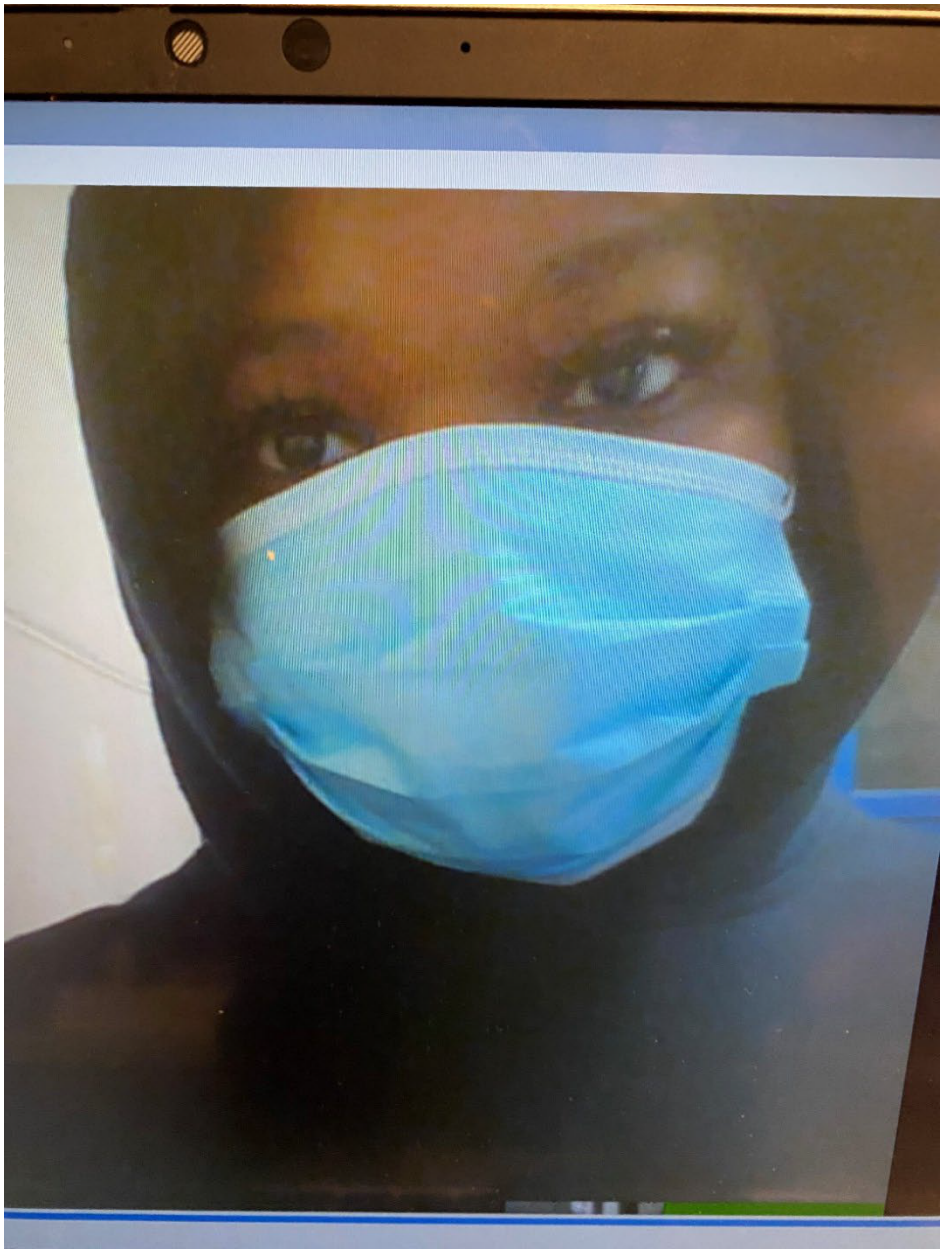
24. At 8:20 pm, a dark sedan arrived at the Marshallton Post Office. The female consistent with Holloway wearing a mask, dark USPS hooded sweatshirt, and tight white shorts

entered Marshallton Post Office and disabled the security alarm—which contained a covert surveillance camera installed by USPS-OIG—using the User 3 access code. The female consistent with Holloway proceeded to the area where Company 1's parcels are stored and opened parcels to review and remove their contents for over 30 minutes. USPS-OIG special agents recorded the thefts on video from a covert surveillance location inside the post office. At 8:51 pm, the female consistent with Holloway placed a phone call from the USPS supervisor desk landline phone and the dark sedan returned to the Marshallton Post Office parking lot. The female consistent with Holloway placed all stolen products in the blue bag she brought from her residence, re-armed the post office's security system, and departed Marshallton Post Office at 8:52 pm.

25. At 9:12 pm, a USPS-OIG special agent witnessed the dark sedan pull up in front of Holloway's residence. The USPS-OIG special agent then witnessed the female consistent with Holloway exit the vehicle carrying the blue bag which appeared heavy and weighted with items. The female consistent with Holloway entered Holloway's residence and the surveillance operation concluded.

26. After the conclusion of the surveillance operation, USPS-OIG agents checked the landline telephone Holloway used to place a call. Agents reviewed the call log and discovered Holloway had dialed which your affiant confirmed through a law enforcement database belongs to . is not a USPS employee and your affiant has not yet ascertained the connection between and Holloway.

27. USPS-OIG special agents also removed the hard drive from the covert surveillance camera that was installed inside the Marshallton Post Office security alarm. Review of that footage provided the following image from the time of the thefts that evening:



28. On June 6, 2022, your affiant showed the photo above to Witness 2. Witness 2 immediately responded "That's Jasmine, without a doubt."

29. As your affiant was conducting the above investigative steps, your affiant was also working to locate the electronic devices stolen from parcels shipped to Company 1. As stated above, Company 1's customers report what they are shipping on Company 1's website, and Company 1 began keeping records of empty parcels it received beginning in August 2021. Through those two logs, your affiant has been able to match up empty parcels with specific stolen items.

30. According to Company 1's records, three Apple laptop computers were stolen from parcels sent to Company 1 in late August 2021. On November 12, 2021, your affiant served an Inspector General (IG) Subpoena to Apple, Inc. for records related to the serial numbers of the three computers. In response, Apple confirmed that all three laptops were activated and in use in either Wilmington, Delaware or Philadelphia, Pennsylvania. One laptop, a 2015 MacBook Pro, was being used by iCloud account "harrisw1218@gmail.com". Apple also gave a registered address for the user of iCloud account harrisw1218@gmail.com in Philadelphia, Pennsylvania.

31. On December 29, 2021, your affiant conducted a consensual interview of the user of iCloud account harrisw1218@gmail.com ("Witness 3") at her residence. Witness 3 stated her ex-boyfriend helped her purchase a 2015 MacBook Pro laptop from an Instagram account titled "We_got_credit." The "We_got_credit" account would post items available for sale at prices lower than market value. The account instructed interested parties only to contact the telephone number associated with an item's post, and never direct message the account regarding items for

sale. The telephone numbers associated with the item for sale posts changed with each post. Witness 3 and her ex-boyfriend contacted "We_got_credit" regarding a 2015 MacBook Pro and were given a location, date, and time to meet. When Witness 3 and her ex-boyfriend arrived at the purchase location, they observed two women and a man selling unpackaged laptop computers out of the back of an SUV. Witness 3 purchased a 2015 MacBook Pro with no charger for $350.00. Your affiant verified that the serial number of the 2015 MacBook Pro in Witness 3's possession matched the serial number of the 2015 MacBook Pro Company 1 reported stolen.

32. On or around January 20, 2022, your affiant served a grand jury subpoena to Facebook, Inc. for records for Instagram account "We_got_credit." Facebook responded with records indicating the registered email address for the "We_got_credit" account is and the verified phone number is Your affiant issued follow-up grand jury subpoenas to identify the users of that email address and telephone number and identified individuals living in Pennsylvania. As such, it appears at least some of the items Holloway removes from the Marshallton Post Office are being sold by associates coordinated through online and telephonic communications.

II. Seizure of the Target Device

33. On June 8, 2022, a United States Magistrate Judge with the United States District Court for the District of Delaware issued a Criminal Complaint charging Holloway with the theft of mail matter, in violation of Title 18, United States Code, Section 1709, as well as an arrest warrant and a warrant to search Holloway's home and her person and to seize, among other items, cellular telephones used by Holloway.

34. On June 9, 2022 at approximately 6:15 am, USPS-OIG special agents arrested Holloway at her residence located at . Once Holloway was in custody, USPS-OIG special agents and USPIS postal inspectors executed a search warrant on the residence, during which they discovered the Target Device.

35. At 7:04 am, USPS-OIG special agents informed Holloway of her Miranda Rights. Holloway stated she understood her rights, waived her rights, and agreed to be interviewed by USPS-OIG special agents at her home. During this interview, Holloway confessed to accessing the Marshallton Post Office after hours on Sunday nights to steal parcels. During Holloway's subject interview, she confirmed the Target Device belonged to her, consented to a limited search of the device, provided the Target Device to law enforcement unlocked, and provided the following information:

a. Holloway's friend Alexis Last Name Unknown (LNU) introduced her to an individual named "Ant" (short for "Antoine") and advised that "Ant" purchased cellphones and other electronics.

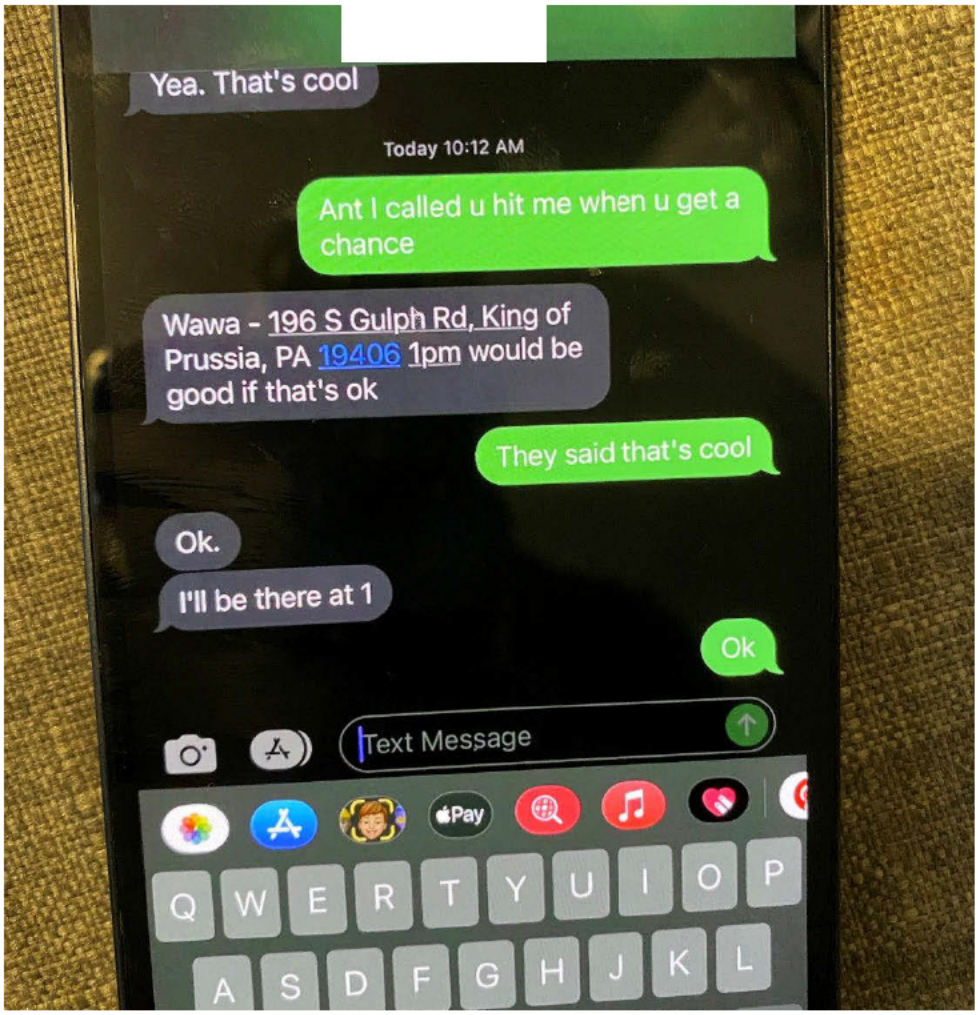
b. Shortly after Holloway became employed by USPS in 2019 at the Marshallton Post Office, she began stealing electronics from parcels there to sell to "Ant."

c. Holloway stated she stole electronics from parcels at the Marshallton Post Office multiple times in 2019 to sell to "Ant," and resumed doing so in 2022.

d. Howell advised her most recent overnight entry to the Marshallton Post Office was on June 5, 2022, and on June 6, 2022, she sold the items she had acquired that night to "Ant."

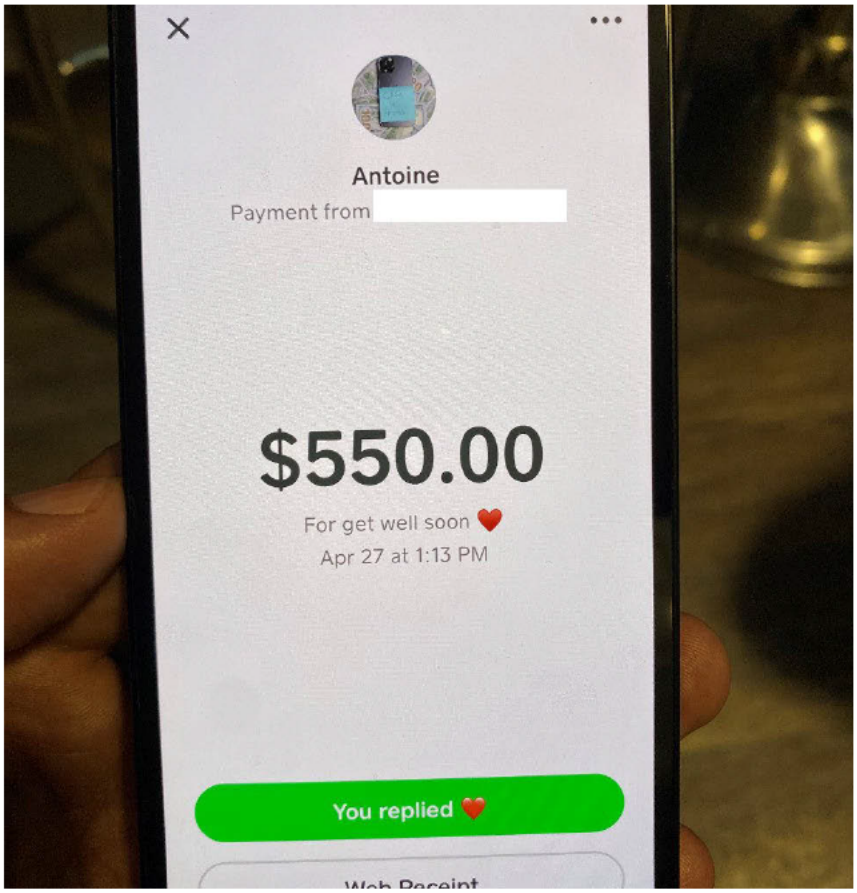
e. Holloway explained the process as: she would steal electronics from the Marshallton Post Office (primarily Apple products) on Sunday night and would then provide the serial numbers of those products to "Ant" once she got home. "Ant" would check the serial numbers using a method unknown to Holloway that would reveal whether the device was clean and able to be activated. "Ant" would then tell Holloway what devices he wanted and give her a time and location to meet the next day. Holloway stated she almost always met "Ant" at the Royal Farms in Broomall, Pennsylvania to sell him the stolen devices. Your affiant conducted research and determined there is a Royal Farms located at 2130 West Chester Pike, Broomall, Pennsylvania 19008. "Ant" would then pay Holloway cash every time at an amount he set based on what devices he purchased from Holloway.

f. Holloway advised she communicated with "Ant" via cellular telephone, although she did not have "Ant's" number saved in her phone. Holloway provided consent for USPS-OIG special agents to review her phone contacts to try and locate a number for "Ant." When the number was unable to be located, Holloway stated she would call Alexis LNU to obtain it. Holloway called Alexis LNU, spoke with her briefly to request "Ant's" phone number, and shortly after that received a text message of a screen shot between Alexis LNU and "Ant" (Ant's phone number is at the top of the screen), see next page:



g. Holloway advised she also received payment from "Ant" through the financial transfer program CashApp on one occasion. Holloway explained someone she knew had electronics to sell several months ago and needed to find a buyer. Holloway told this individual she had a buyer and contacted "Ant" with the information about the electronics. "Ant" said he would purchase the electronics for $2,000.00. Holloway told "Ant" she was going to tell the individual with the electronics the price was $1,500.00 and she would keep the extra $500.00. "Ant"

then sent Holloway a payment on CashApp for $550.00 once the transaction was complete. Holloway provided consent for USPS-OIG special agents to review her CashApp transaction history. Your affiant located the relevant transaction which revealed Holloway received a $550.00 payment from "Antoine" on April 27, 2022 at 1:13PM. "Antoine's" CashApp user name is see next page:



36. Based on Holloway's confession to repeated mail thefts from Marshallton Post Office, Holloway's consent for a limited review of the contents of her cellphone, and the

discovery of evidence on that iPhone relevant to the associated criminal conduct, your affiant has probable cause to believe Holloway is engaged in a scheme to steal mail matter from a U.S. Post Office and that additional evidence of criminal activity is located within the Target Device, including but not limited to correspondence with coconspirators, descriptions of stolen devices, and evidence of Holloway's compensation for stolen devices.

TECHNICAL TERMS

37. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly

transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is,

long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

38. Based on my training and experience, while your affiant has not yet been able to determine the model of cellular telephone possessed by Holloway, your affiant knows that telephones at least have the ability to serve as wireless telephones, and that most also have the ability to serve as a digital camera, portable media player, GPS, and PDA. In my training and experience, examining data stored on cellular telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the device, that person's contacts, photos, and location.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

39. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

a cellular telephone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to communicate with coconspirators or otherwise further an offense, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

42. I submit that this affidavit supports probable cause for a warrant to search the Target Device described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Justin Lynch
Special Agent
U.S. Postal Service
Office of Inspector General

Subscribed and sworn to before me by telephone pursuant to Fed.R.Crim.P. Rules 4.1 & 41(d)(3).

on June 10, 2022

HONORABLE SHERRY R. FALLON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

A black iPhone 12 with IMEI number 352590374630790, currently stored in an evidence package within the possession of USPS-OIG SA Justin Lynch in the District of Delaware. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, United States Code, Section 1709 (Theft of Mail Matter by Postal Employee), those violations involving Jasmine Holloway and occurring after August 1, 2021, including:

a. evidence of who used, owned, or controlled the Telephone at the time of the events described in this warrant, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of the theft of mail matter, including but not limited to photos or descriptions of stolen items and communications with associates about the theft and/or resale of stolen items;

c. evidence of Holloway's location at times when the theft of mail matter occurred;

d. evidence of Holloway's compensation for stolen items;

e. records of or information about the Telephone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

f. evidence indicating the Telephone user's state of mind as it relates to the crime under investigation;

g. passwords, encryption keys, and other access devices that may be necessary to access the Telephone;

h. records of or information about Internet Protocol addresses used by the Telephone;

i. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.